Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106
	)	

To: The Commission

REPLY COMMENTS AND ADDITIONAL COMMENTS ON THE INITIAL REGULATORY FLEXIBILITY ANALYSIS OF THE WIRELESS INTERNET SERVICE PROVIDERS ASSOCIATION

Stephen E. Coran
S. Jenell Trigg
Deborah J. Salons
Lerman Senter PLLC
2001 L Street, N.W., Suite 400
Washington, D.C. 20036
(202) 429-8970
Counsel to the Wireless Internet Service Providers Association

July 6, 2016

TABLE OF CONTENTS

Summary

Not unlike the discussion over the Open Internet rules that devolved into an ideological debate between parties favoring regulation to ban predictive behavior and those seeking maintenance of a successful "light touch" regulatory approach, this proceeding pits polarizing forces against each other – so-called privacy advocates and large broadband providers. But there is a third stakeholder that cannot be ignored – small broadband providers that lack the resources to comply with an extensive set of rules that, in the words of the U.S. Small Business Administration's Office of Advocacy, "would have significantly disproportionate economic impacts on small BIAS providers if finalized."[*] These economic impacts also would adversely affect broadband customers that would see increased bills and rural Americans that will remain outside the reach of terrestrial broadband networks as investment and innovation declines.

The Wireless Internet Service Providers Association ("WISPA"), an organization that represents the interests of small fixed broadband providers, replies to certain of the Comments in the record. WISPA fully supports the protection of customer personally identifiable information ("PII"), but by reasonable means that reflect how the Internet works, the distinct roles of the various members of the ecosystem, and the need for flexibility given the different sizes and scale of broadband Internet access service providers. Overall, the record demonstrates strong support for adopting a flexible regulatory approach coupled with relief for small providers that defers application of new rules, grandfathers existing privacy policies and exempts certain proposed obligations. In particular, organizations representing small providers agree on a number of points, and initial Comments do not appear to challenge the view that small providers must obtain relief from the proposed rules, should they be adopted.

[*] *See* Reply Comments of the U.S. Small Business Administration Office of Advocacy, WC Docket No. 16-106 (filed June 27, 2017) at 2.

As a threshold matter, the record demonstrates that the Commission's proposals exceed the scope of its statutory authority. Numerous commenters agree that Section 222 of the Communications Act of 1934, as amended, limits the Commission's authority to protecting Customer Proprietary Network Information ("CPNI"), and the more general terms of Sections 201, 202 and 706 cannot, as a matter of statutory construction, form the basis for rules that seek to protect what the Commission calls "customer proprietary information."

But even if the Commission has authority, that does not mean that the Commission *should* exercise it with prescriptive and burdensome rules. Rather, as many commenters have urged, the Commission should adopt the Industry Framework that will provide broadband providers with flexibility in the methods it employs to protect their customers from unfair and deceptive practices.

As examples of the excessive nature of the proposed rules, numerous commenters (including the staff of the Federal Trade Commission's Bureau of Consumer Protection) point out that some of the proposed definitions would impose significant obligations on broadband providers, with little or no benefit to consumers. For example, requiring notification of unintentional data security breaches that impose no actual harm or risk of harm to the consumer would be totally unreasonable, unnecessary and will lead to notice fatigue and confusion among customers. There is no legitimate reason to treat former customers and applicants in the same manner as existing customers. The Commission's proposed rules also do not distinguish between sensitive and non-sensitive information, which would increase record-keeping obligations and raise compliance risk for inconsequential privacy breaches.

But the real issue here for WISPA and its members is that the proposed rules would apply across the board, with little consideration of the size of the provider. The record demonstrates

that small providers – many with a handful of staff that serve a few hundred customers in areas where other terrestrial broadband options are not available – will be disproportionately harmed. On limited budgets where scarce financial and human resources are best spent on upgrading and expanding networks, they simply cannot absorb additional estimated annual costs of $130-200 per customer record without investment and deployment being materially and negatively affected. To do the math, a $150 per-customer cost for each data breach notification would, for each data breach incident, divert $75,000 away from investment that could otherwise be used to double the number of subscribers on a 500-subscriber WISP network.

This proceeding cannot be viewed in a vacuum. The proposed privacy rules would be cumulative with the Commission's imposition of Title II regulations and enforcement under its *2015 Open Internet Order*, with additional transparency obligations if the small business exemption is not made permanent, and any additional requirements imposed by the Commission's new rulemaking regarding outage reporting. This grand slam of regulations within a short amount of time compounds the significant economic impact imposed on a substantial number of small broadband providers.

The record demonstrates support for a number of industry proposals that will soften the blow of excessive regulation of small businesses. First, several commenters urge the Commission to extend the deadline for compliance for up to two years, with further proceedings to determine whether the deadline should be further extended and if other relief is warranted. Without sufficient time, small providers simply cannot budget for the salaries of new personnel, lawyers and other compliance costs. Second, small providers' existing privacy policies should be grandfathered. Third, the Commission should permanently exempt small providers from the

subsections of proposed Section 64.7005(a), and the size of the provider should be an express consideration in proposed Section 64.7005(b).

The impact of the Commission's proposed broadband privacy rules on small providers must not be lost amid the *Sturm und Drang* of this proceeding. For small broadband providers that are facing an entirely new Title II regulatory regime with a host of new legal obligations, the stakes are high and the consequences real. The Commission must follow the record and adopt rules that will not impair the ability of small providers to continue to provide affordable fixed broadband service.

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106
	)	

To: The Commission

REPLY COMMENTS
AND ADDITIONAL COMMENTS ON
THE INITIAL REGULATORY FLEXIBILITY ANALYSIS OF
THE WIRELESS INTERNET SERVICE PROVIDERS ASSOCIATION

The Wireless Internet Service Providers Association ("WISPA"), pursuant to Sections 1.415 and 1.419 of the Commission's Rules, hereby replies to certain of the initial Comments filed in the above-referenced proceeding.[1]

The Comments filed by broadband providers and their trade associations uniformly agree that the Commission's proposed rules would, if adopted, constitute an overly prescriptive and unnecessary regulatory regime that would exceed the authority Congress delegated to the Commission and would impose significant costs and burdens on providers, especially small providers that lack the resources necessary to comply. Although the Commission professes a desire "to provide flexibility for small providers whenever possible,"[2] the proposed rules make no distinction between large providers and small providers, which would be forced to divert resources away from investment and deployment to rural, unserved and underserved Americans

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, WC Docket No. 16-106, 31 FCC Rcd 2500 (rel. April 1, 2016) ("*NPRM*"). WISPA filed Comments in response to the *NPRM*. *See generally* Comments of WISPA, WC Docket No. 16-106 (filed May 27, 2016) ("WISPA Comments").

[2] *See NPRM* at Appendix B, Initial Regulatory Flexibility Analysis ("IRFA") at ¶ 56.

to hiring staff and establishing rigid procedures to comply with the rules.[3] The "one size fits all" regime would be a prescription for failure that could leave unserved Americans on the broadband sidelines. By contrast, a flexible regulatory approach coupled with specific small business benefits would help avoid such a result while assuring adequate protection of consumers' legitimate privacy interests.

Certain commenters do not demonstrate appreciation for market realities, especially those faced by small broadband providers, and instead would treat all broadband providers as if they possess market power. Some fail to consider the tremendous costs and burdens that would accompany new record-keeping, staffing and training, disclosure and reporting obligations. Other commenters simply assume that broadband providers can continue doing business in an uncertain climate where the understanding of what is "reasonable" and what is not, and the vagaries of the regulatory and enforcement system, elevate risk, deter innovation and chill new investment.

WISPA is pleased that commenters representing the interests of broadband providers have echoed WISPA's call for rules that would defer the deadline for compliance with new requirements and exempt small broadband providers from certain rules. In particular, allowing small providers more time to comply would enable them to budget for the additional costs, determine how much to increase their customers' bills, and afford the Commission and the public time to consider whether further relief would be necessary. Commenters also

[3] Missing from the IRFA is any discussion of fixed broadband providers that rely on unlicensed spectrum. The IRFA includes several paragraphs discussing cable, satellite and a number of various licensed bands, but the Commission conceded that it has "no specific information on the number of small entities that provide broadband service over unlicensed spectrum." *Id.* at ¶ 9. Although the Commission professes to include such providers in its IRFA, the lack of any industry data renders the WISP industry an afterthought and the IRFA deficient. As a starting point, given its continuing unwillingness to collect data, the Commission could rely on its Form 477 data and on WISPA's estimates of approximately 2,500 fixed wireless Internet service providers that serve three million consumers.

recommended that small providers' privacy policies be grandfathered and that they be permanently exempt from certain implementation requirements.

Our nation and economy have been built on the backs of small businesses. As President Obama acknowledged, "[s]mall businesses play an essential role in the American economy; they help fuel productivity, economic growth, and job creation."[4] Small providers have deployed fixed broadband service in small towns and urban and rural communities that would be unserved today if not for their foresight, ingenuity, innovation and investment. That entrepreneurial spirit and the benefits to the public that small broadband providers bring have grown in part from the regulatory "light touch" the Commission employed until it adopted the *2015 Open Internet Order*[5] and began a campaign to impose heavy-handed Open Internet, privacy and outage reporting regulations on broadband providers, large and small.[6]

A primary question in this proceeding is one of degree – what *should* the Commission do to protect consumers' legitimate privacy interests without discouraging investment and deployment? Guidance rests in the views expressed in this proceeding by two other federal agencies. The Federal Trade Commission's Bureau of Consumer Protection ("FTC") described a number of improvements to the Commission's proposed rules that would reduce regulatory

---

[4] Presidential Memorandum of January 18, 2011, *Regulatory Flexibility, Small Business, and Job Creation, Memorandum for the Heads of Executive Departments and Agencies*, 76 Fed. Reg. 3827, 3827 (Jan. 21, 2011) (citing to the Regulatory Flexibility Act, which establishes a "deep national commitment" to achieving statutory goals without unnecessary burdens on the public") ("Presidential Memorandum"). This Presidential Memorandum was issued concurrently with Executive Order 13563, which reinforced the importance of compliance with the Regulatory Flexibility Act ("RFA") by all federal agencies. *See* 76 Fed. Reg. 3821 (Jan. 21, 2011). President Obama issued subsequent Executive Order 13579 that expressly imposed the obligations of Executive Order 13563 on independent regulatory agencies. *See* 76 Fed. Reg. 41587, § 1(c) (July 14, 2011) ("Executive Order 13563 set out general requirements directed to executive agencies concerning public participation, integration and innovation, flexible approaches, and science. To the extent permitted by law, independent regulatory agencies should comply with these provisions as well").

[5] *See Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (2015) ("*2015 Open Internet Order*").

[6] *See, e.g., Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications*, Report and Order, Further Notice of Proposed Rulemaking, and Order on Reconsideration, PS Docket No. 15-80, FCC 16-63 (rel. May 26, 2016) (proposing to require broadband providers to report service disruptions "that would result in the loss of any user functionality").

burdens on broadband providers and eliminate many of prescriptive elements.[7] The FTC also has recognized that in certain situations the burden that additional privacy requirements "impose on small businesses" outweighs "the reduced risk of harm from the collection and use of limited amounts of non-sensitive consumer data."[8] The U.S. Small Business Administration's Office of Advocacy ("Advocacy") declared that the proposed rules "would have significantly disproportionate economic impacts on small BIAS providers if finalized," exposed a lack of any paperwork burden estimates and endorsed a number of measures to mitigate the economic effects on small businesses.[9]

---

[7] *See* Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, WC Docket No. 16-106 (filed May 27, 2016) ("FTC Staff Comments").

[8] Federal Trade Comm'n, Protecting Consumer Privacy In An Era Of Rapid Change: Recommendations For Businesses And Policymakers 15 (Mar. 2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-reportprotecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[9] Reply Comments of the U.S. Small Business Administration Office of Advocacy, WC Docket No. 16-106 (filed June 27, 2017) ("Advocacy Reply Comments") at 2. *See also United States Telecom Ass'n v. FCC*, 2016 U.S. App. LEXIS 10716 (D.C. Cir. June 14, 2016) ("*USTelecom*") at 64-65 (Williams, J., dissenting):

> The palliative effect of these procedures may be considerable for the very large service providers. They are surely accustomed to having their lawyers suit up, research all the angles, participate in proceedings after notice has been given to all potentially adversely affected parties, and receive, after an indefinite stretch, a green light or a red one. *For the smaller fry, the internet service provider firms whose growth is likely to depend on innovative business models (precisely the sort that seem likely to run afoul of the Commission's broad prescriptions*; see part II.B), the slow and costly advisory procedure will provide only a mild antidote to those prescriptions' negative effect. *This of course fits the general pattern of regulation's being more burdensome for small firms than for large, as larger firms can spread regulation's fixed costs over more units of output.* The palliative effect of these procedures may be considerable for the very large service providers. They are surely accustomed to having their lawyers suit up, research all the angles, participate in proceedings after notice has been given to all potentially adversely affected parties, and receive, after an indefinite stretch, a green light or a red one. *For the smaller fry, the internet service provider firms whose growth is likely to depend on innovative business models (precisely the sort that seem likely to run afoul of the Commission's broad prescriptions*; see part II.B), the slow and costly advisory procedure will provide only a mild antidote to those prescriptions' negative effect. *This of course fits the general pattern of regulation's being more burdensome for small firms than for large, as larger firms can spread regulation's fixed costs over more units of output.*

(Emphases added). Although Judge Williams was writing about the advisory opinion process, his opinion stands for the broader proposition that small broadband providers lack the resources of larger ones and therefore assume greater relative compliance burdens and risk. President Obama also emphasized the "importance of recognizing 'differences in the scale and resources of regulated entities' and of considering 'alternative regulatory approaches . . . which minimize the significant economic impact of rules on small businesses, small organizations, and small governmental jurisdictions.'" Presidential Memorandum, 76 Fed. Reg. 3827.

Many of the measures Advocacy recommended cite the specific proposals of WISPA and other commenters on how the Commission can minimize the disproportionate affects the proposed regulations will have on small businesses and can better balance the privacy interests of consumers and the small companies that serve them. In addition to adopting the flexible Industry Framework that is based on the FTC Act,[10] the Commission should adopt additional relief that would eliminate the significant economic impact its prescriptive and burdensome proposed rules would impose on small broadband providers.

Discussion

In November 2014, Chairman Wheeler stated that: "Let me be crystal clear on this point: I do not believe that a compliance checklist is the right answer for cyber risk management. Rather, I want companies to develop a *dynamic strategy that can be both more effective and more adaptive than a traditional prescriptive regulatory approach*."[11] In the IRFA, the Commission stated that "in formulating these rules, *we seek to provide flexibility for small providers whenever possible, by setting out standards and goals for the providers to reach in whichever way is most efficient for them*."[12] But in sharp contrast to these statements, the Commission has done the opposite, proposing detailed and prescriptive rules that allow little margin for dynamism, adaptation, standards and goals, and which would disproportionately harm small providers and the customers they serve.

WISPA respects the fact that broadband customers have legitimate privacy interests that must be protected through privacy policies and procedures intended to promote choice,

[10] *See* Letter from Matthew M. Polka, President & CEO, ACA, *et al.*, to The Honorable Tom Wheeler, Chairman, FCC (Mar. 1, 2016) (on file with WCB) (Privacy Framework Discussion Paper attached to the letter will be referred to herein as the "Industry Framework").
[11] *See* Comments of The United State Telecom Association, WC Docket No. 16-106 (filed May 27, 2016) ("USTelecom Comments") at 26, *citing* Remarks of Chairman Wheeler, November 2014 *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-330574A1.pdf (emphasis added).
[12] IRFA at ¶ 56 (emphasis added).

transparency and data security. WISPA's members are mindful of these principles and take seriously their obligations to the welfare of the small and rural communities they serve. In considering the record in this proceeding, WISPA urges the Commission to account for the interests of small broadband providers by adopting generally applicable adaptive and flexible rules.

I. THE RECORD DEMONSTRATES THAT THE COMMISSION DOES NOT HAVE STATUTORY AUTHORITY TO ADOPT THE PROPOSED RULES.

A. The Commission's Authority Under Sections 201 And 202 Is Limited.

Sections 201 and 202 are not independent sources of authority, but rather rules of general application that cannot be construed to permit the Commission to regulate broadband CPNI.[13] Although Free Press may be correct in stating that "Sections 201 and 202's prescriptions are by congressional design both more expansive and less specific than the privacy rules mandated by Section 222,"[14] this helps prove the rule of statutory construction that USTelecom paraphrased: "where Congress has covered a topic in a more specific provision, an agency may not find authority to expand on that topic in a more general provision."[15] The American Cable Association ("ACA") recognized that the Commission itself applied this principle in its *1999 CPNI Order on Reconsideration*, stating that "the specific consumer privacy and consumer

[13] *See, e.g.*, WISPA Comments at 6; Comments of the Consumer Technology Association f/k/a The Consumer Electronics Association, WC Docket No. 16-106 (filed May 27, 2016) ("CTA Comments") at 7; Comments of Verizon, WC Docket No. 16-106 (filed May 27, 2016) ("Verizon Comments") at 60; Comments of CTIA, WC Docket No. 16-106 (filed May 27, 2016) ("CTIA Comments") at 60-62; Comments of Washington Legal Foundation, WC Docket No. 16-106 (filed May 27, 2016) ("WLF Comments") at 4.

[14] Comments of Free Press, WC Docket No. 16-106 (filed May 27, 2016) ("Free Press Comments") at 15.

[15] USTelecom Comments at 33. *See also* Verizon Comments at 60-61, *citing Fourco Glass Co. v. Transmirra Prods. Corp.*, 353 U.S. 222, 228-229 (1957) ("However inclusive may be the general language of a statute, it will not be held to apply to a matter specifically dealt with in another part of the same enactment. Specific terms prevail over the general in the same or another statue which otherwise might be controlling").

choice protections established in section 222 supersede the general protections identified in section 201(b) and 202 (a)."[16]

The Commission cannot now deviate from well-settled principles of statutory construction and its own precedent to contrive authority where it does not exist.[17] As the Washington Legal Foundation described, the Commission "apparently believes that if it merely cites enough possible sources of statutory authority – if its grasps at enough straws – then a reviewing court may be more likely to defer to the agency on review. But no amount of thin reeds will save the agency's argument."[18]

B. Section 222 Does Not Confer Authority To Impose Privacy Rules On Broadband Providers.

The Comments demonstrate that the Commission's regulatory authority also is extremely limited by the plain language of Section 222, "a provision that expressly applies only to voice telephony services, and relying on other broadly worded, general statutory provisions to impose onerous, far reaching, and discriminatory requirements on only some Internet-related service providers, the Commission proposes to take action that would be arbitrary, capricious, and beyond the scope of its statutory authority."[19]

The Congressional intent behind the passage of Section 222 was to regulate voice telephony services.[20] As USTelecom explained, "the traditional privacy requirements that

[16] Comments of American Cable Association, WC Docket No. 16-106 (filed May 27, 2016) ("ACA Comments") at 17, *citing Implementation of the Telecommunications Act of 1996, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended*, CC Docket Nos. 96-115, 96-149, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, 14490-91 (rel. Sept. 3, 1999) ("*1999 CPNI Order on Reconsideration*").
[17] *See* US Telecom Comments at 27-28, 32-33.
[18] WLF Comments at 4.
[19] USTelecom Comments at 28.
[20] *See id. See also* Comments of National Cable & Telecommunications Association, WC Docket No. 16-106 (filed May 27, 2016) ("NCTA Comments") at 7-13; Comments of the American Advertising Federation, *et al.*, WC Docket No. 16-106 (filed May 27, 2016) at 5.

Congress delineated in Section 222 were assembled based on concerns that could arise in the single platform, monopoly provider world of voice-only communications"[21] and that "Section 222 does not, by its terms, extend to protect the privacy of customer information for services other than voice telephony services."[22] Rather, the Commission should await specific direction from Congress before it can extend its privacy protection rules beyond the specific confines of Section 222. Although protections of consumers' privacy interests are essential, so, too, is the limit of the agency's authority.

The WISPA Comments also pointed out a serious flaw in the Commission's proposed scheme – the vast expansion of the universe of information that would require protection.[23] Rather than using the existing definition of CPNI and adapting it to reflect the inherent differences between a customer's private voice and broadband information, the Commission proposes to classify information that would be protected as *customer proprietary information*,[24] a newly contrived term that the Commission defines as "private information that customers have an interest in protecting from public disclosure," including both: 1) CPNI, *and* 2) PII collected by providers through their provision of broadband service.[25]

Several industry commenters agree with WISPA that the Commission lacks authority to extend its rules beyond the protection of CPNI.[26] As CTIA clearly stated, "the text and structure

[21] USTelecom Comments at 3-4.
[22] *Id.* at 28.
[23] *See* WISPA Comments at 12-13.
[24] The Commission abbreviates this term to "Customer PI" in the *NPRM*, although "PI" is generally understood to mean "personal information" and not "proprietary information." Notwithstanding, the term "customer proprietary information" is used in these Reply Comments in order to discuss the contents of the Commission's proposal. *See NPRM* at 2507.
[25] *See id.* at 2519.
[26] *See* CTA Comments at 6 ("[t]his interpretation of Section 222(a), which expands the scope of customer data protection beyond CPNI, conflicts with the language, structure, and purpose of Section 222 and contravenes Congress's intent in enacting Section 222"); Comments of ITTA, WC Docket No. 16-106 (filed May 27, 2016) ("ITTA Comments") at 11, *citing Util. Air Regulatory Grp v. EPA*, 134 S. Ct. 2427, 2446 (2014) ("[t]he NPRM takes a revisionist, result-driven approach that runs afoul of cardinal rules of statutory interpretation and the

of Section 222, as well as its legislative history, make clear that CPNI is the *only* customer data that Section 222 protects."[27] NTCA likewise observed that "[n]either 'PII' nor the collective 'customer proprietary information' category proposed by the Commission appear in the statute, and neither does the statute confer upon the Commission authority to create such categories."[28] Simply put, "[s]ection 222(a) only refers to CPNI and only provides authority to regulate CPNI, not some broader category of information that the Commission seems intent on creating here."[29] Indeed, the term "Customer Proprietary Information" does not appear anywhere in the Act, but is a term "the Commission apparently invented in its 2014 Notice of Apparent Liability against TerraCom and YourTel."[30]

Ignoring the obvious, public interest groups cite two purported sources of authority. First, EFF asserted that broadband providers have a "*general duty* of a telecommunications carrier that extends beyond just CPNI and applies to all information that includes PII as well (collectively referred to as customer PI)."[31] Second, they "agree with the Commission's proposal to cover both CPNI and PII as customer proprietary information or 'customer PI' under the *TerraCom NAL*."[32] But the Commission cannot just conjure up authority based on a "general

---

Commission's own long-held adherence to its governing law"); NCTA Comments at 8-9; Comments of Mobile Future, WC Docket No. 16-106 (filed May 27, 2016) ("Mobile Future Comments") at 13.

[27] CTIA Comments at 25.

[28] Comments of NTCA—The Rural Broadband Association, WC Docket No. 16-106 (filed May 27, 2016) ("NTCA Comments") at 27. *See also* USTelecom Comments at 7-8 ("the Notice proposes to go far beyond these traditional words defining CPNI, attempting to create a new term 'Customer PI'" which would "a massive expansion of the concept of CPNI...untethered to the statute").

[29] *Id.* at 8. Moreover, as USTelecom stated, "the Commission is also without authority to expand the definition of CPNI…. [a]n agency cannot reinterpret a defined term that is specific and clear, and that contains no qualifying language such as 'including…' or 'among other things…" to extend its regulatory reach." *Id.* at 30. As Sprint noted, "[s]uch an expansion is inconsistent with the plain language and structure of Section 222 and…the Commission's statutory authority to regulate data privacy and security." Comments of Sprint Corporation, WC Docket No. 16-106 (filed May 27, 2016) ("Sprint Comments") at 5.

[30] ACA Comments at 13, *citing TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13330 (2014).

[31] Comments of The Electronic Frontier Foundation, WC Docket No. 16-106 (filed May 27, 2016) ("EFF Comments") at 2 (emphasis added).

[32] *Id.* at 4. *See also* Comments of the International Center for Law and Economics and Scholars of Law and Economics, WC Docket No. 16-106 (filed May 27, 2016) at 3; Free Press Comments at 11.

duty" that cannot be found in the statute and which opens the door for virtually any kind of information to be subject to protection. And a Notice of Apparent Liability in an adjudicatory enforcement proceeding against individual parties in which the Commission ignored its previous longstanding position regarding Section 222 should not confer authority to a broad class of providers.[33] These claims of authority thus are unfounded.

Even worse, several public advocacy groups suggested that the term "customer proprietary information" should remain open and loosely defined. New America recommended that "customer PI should remain an open category" so that "[a]s BIAS providers further develop their services, new types of data may need to be categorized as CPNI or PII, and thus will merit protection under the FCC's scheme."[34] EFF simply contended "that the FCC provide an illustrative but not exhaustive list of examples to the industry to update it frequently as technology changes to reduce compliance costs and avoid obsolescence."[35] Such an open-ended approach creates significant ambiguity in the marketplace and gives the Commission regulatory fiat to make up the rules as it goes along, without providing broadband providers and consumers with certainty about what information must to be protected. The Commission should not give itself the ability to arbitrarily "update" a list of examples at its whim and expect it to have the force of law.[36]

[33] *See* CTA Comment at 6, n.14.
[34] Comments of New America's Open Technology Institute, WC Docket No. 16-106 (filed May 27, 2016) ("New America Comments") at 22.
[35] EFF Comments at 19.
[36] *See* Comments of Richard Bennett, WC Docket No. 16-106 (filed May 27, 2016) at 8 ("CPNI is not a bludgeon to be used arbitrarily").

C. Section 706 Is Not A Source Of Statutory Authority For Imposing Privacy Or Data Security Regulations, But It Does Provide Ample Statutory Authority To Provide Regulatory Relief To Small Broadband Providers.

Section 706 of the Telecommunications Act of 1996 ("Telecom Act") mandates the Commission to "take immediate action to accelerate deployment of such capability by *removing barriers to infrastructure investment and by promoting competition in the telecommunications market.*"[37] WISPA and other commenters showed that the proposed rules would contravene that statutory precept – a prescriptive and onerous privacy regulation scheme will add barriers, discourage deployment, and hamper competition, contrary to the plain language of the statute.[38] The "virtuous cycle" the Commission recites is at best speculative "because the rules have the *potential* to increase customer confidence in BIAS providers' practices, that *might* lead to a boost in customer confidence, which *could* lead to an increase in the use of broadband, which *should* then encourage deployment."[39] WISPA agrees that "[t]his tortured path makes clear that the proposed rules are several steps removed from anything that could plausibly have a direct and meaningful impact on deployment."[40]

Far less speculative is the unassailable fact that there will be significant costs associated with overall compliance, and that small providers will be disproportionately and negatively affected to the detriment of their customers. As ACA explained, the proposed rules would: 1) divert scare resources from deployment, network improvement, and customer service to regulatory compliance; 2) undermine the trust in the broadband ecosystem by fatiguing customers through a deluge of notification and opt-out/opt-in choices, and by creating an uneven

[37] Pub. L. No. 104-104 (Feb. 8, 1996), *codified as* 47 U.S.C. § 1302(b) (emphasis added).
[38] WISPA Comments at 7. *See also* Comments of Free State Foundation, WC Docket No. 16-106 (filed May 27, 2016) at 8; WLF Comments at 8. The Commission also has a statutory duty under Section 257 of the Communications Act of 1934, as amended ("Act") to identify and eliminate market entry barriers for small businesses. 47 U.S.C. § 257.
[39] USTelecom Comments at 35.
[40] *Id.*

playing field between broadband and edge providers; 3) create a drag on broadband deployment , resulting in slow consumer demand that will slow edge provider innovation; and 4) raise barriers to edge provider innovation by requiring broadband providers to obtain opt-in consent from their customers before sharing any customer proprietary information with edge providers.[41]

WISPA agrees with ACA that the proposed rules are "the virtuous cycle in reverse."[42] Small broadband providers that cannot tolerate or absorb the increased costs and regulatory burdens will simply go out of business, leaving their customers with fewer or no alternatives to broadband access. Under any definition, the exit of small broadband providers that deploy cost-effective broadband services to unserved or underserved communities is a *loss of competition* that contravenes the Section 706 mandate to *promote competition*.

II. ALTHOUGH THE DC CIRCUIT HELD THAT THE COMMISSION HAS AUTHORITY TO REGULATE BROADBAND PROVIDERS UNDER TITLE II, THE COMMISSION SHOULD BE CONSISTENT WITH THE FTC'S REGULATORY APPROACH REGARDING PRIVACY AND DATA SECURITY.

A. The Record Supports The FTC-Based Industry Framework.

The record reflects widespread support for the Industry Framework, which is based on the FTC's decades of extensive experience in privacy and data security policy and enforcement

[41] *See* ACA Comments at 21- 22.

[42] *Id.* at 22. *See also* Comments of Electronic Privacy Information Center, WC Docket No. 16-106 (filed May 27, 2016) ("EPIC Comments") at 29. EPIC alleged two studies support how the Commission's proposed rules "align with the virtuous cycle of section 706." *Id.* First, it referenced the 2016 Broadband Progress Report, which acknowledged the Commission "found a correlation exists between non-adoption of broadband security and privacy concerns." *Id.* (*citing 2016 Broadband Progress Report*, 31 FCC Rcd 699, 752 n.35). EPIC also referenced a recent study by the National Telecommunications and Information Administration ("NTIA") that "confirms the FCC's conclusion that privacy concerns impact consumer Internet usage. This allegation is misleading; these studies show how privacy and security impact Internet *adoption* and *usage*- not how the proposed rules will satisfy the FCC's duty to which it "*encourage the deployment* on a reasonable and timely basis of advanced communications" and to "take immediate action to accelerate deployment of such capability by *removing barriers* to infrastructure investment and promoting competition." *Id.* (*citing* Section 706 of the Telecom Act, 47 U.S.C. § 1302(a) and (b)).

for Internet and new technology companies.[43] Instead of specifying detailed, prescriptive and over-reaching rules, the Industry Framework adopts the FTC's "unfair" and "deceptive" approach to privacy and data security, an approach that commenters favored. For example, ITTA stated that "the Commission should carefully consider the Industry Framework, and in any event adopt rules, policies and enforcement practices for BIAS that are technology and competitor-neutral and modeled after the FTC's well-tested and successful privacy and data security regime."[44] Mobile Future referenced the Industry Framework in recommending that "[i]nstead of pursuing its ill-advised proposal, the Commission should work towards harmonizing the FCC rules with the FTC's proven approach."[45] Sprint stated that the Industry Framework "would continue to best protect consumers and ensure that common ground rules apply consistently and fairly to all players in the Internet ecosystem."[46] Verizon agreed that that the Industry Framework would benefit consumers as it "ensures consumers will be afforded a consistent level of protection across the Internet" by "giv[ing] consumers easy-to-understand choices for non-contextual uses of their data, taking into account the sensitivity of data and the context in which the data is collected."[47] Comcast explained that the Industry Framework would "allow the FCC to replicate the successful privacy policies advocated by the Administration and enforced by the FTC by focusing on transparency, choice, data security, data breach notification, and other key principles."[48]

Rather than abandoning the FTC model as the Commission proposes, the Commission should embrace the views of the agency with experience in privacy and data security regulation

[43] *See* Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, WC Docket No. 16-106 (filed May 27, 2016) ("FTC Staff Comments") at 3. *See* Industry Framework ("[t]he FCC's rules and principles for regulating and enforcing privacy and security should be as similar as possible to the FTC approach").
[44] ITTA Comments at 17.
[45] Mobile Future Comments at 2.
[46] Sprint Comments at 2.
[47] Verizon Comments at 7 (citation omitted).
[48] Comments of Comcast Corporation, WC Docket No. 16-106 (filed May 27, 2016) at 3.

and follow the widespread support that approach has in the record. Indeed, the Industry Framework is consistent with Chairman Wheeler's own words: "I want companies to develop a *dynamic strategy that can be both more effective and more adaptive than a traditional prescriptive regulatory approach*."[49]

Not surprisingly, the FTC Staff Comments were critical of the Commission's proposed approach. The FTC shares WISPA's concerns and those of other commenters that describe the Commission's proposed regulatory scheme as too complex, unreasonably focused on broadband providers instead of the entire Internet ecosystem, and not realistically reflective how the Internet operates. The FTC acknowledged that the Commission's proposed rules "would impose a number of specific requirements on the provision of BIAS service that would not generally apply to other services that collect and use significant amounts of consumer data. *This outcome is not optimal.*"[50] Or, as FTC Commissioner Ohlhausen stated, "[t]he [FTC Staff] comment dryly describes the disparity as 'non optimal.' Let me be a bit more explicit: these proposed rules would hamper ISPs from competing with other businesses to serve consumers in data-drive industries, including online advertising….This barrier to competition could be large because the differences between the FCC and FTC approaches are significant."[51] Through the years, the FTC has advocated for baseline privacy and data security protection, as well as security beach notification laws for *all* entities that collect consumer data, and believes that such "generally applicable laws are needed to ensure appropriate protections for consumer's privacy and data security across the marketplace."[52]

---

[49] *See* note 11, *supra*.
[50] FTC Staff Comments at 8 (emphasis added).
[51] FTC Cmmr. Ohlhausen Advertising and Privacy Law Summit Remarks ("Ohlhausen Remarks") at 6.
[52] *Id. See also* Comments of The Rural Wireless Association, Inc., WC Docket No. 16-106 (filed May 27, 2016) ("RWA Comments") at 1 ("prescriptive one-size-fits-all privacy regime applicable only to BIAS providers and not the other entities in the Internet space could place untenable demands and costs on rural wireless broadband providers that are already struggling to provide wireless broadband services in rural and remote areas").

In sum, the FTC Staff Comments confirm what the Industry Framework advocated and what WISPA and others have shown – that by seeking to impose on broadband providers a detailed and prescriptive regulatory regime, the Commission has forgotten what is best for consumers. As discussed in detail below, the Commission should reconsider its initial views, follow the record and adopt rules that effectively protect consumers from actual harms.

B. Broadband Providers Should Not Be Regulated Differently Than Others In The Internet Ecosystem.

Unlike the Commission which would impose privacy regulations only on broadband providers, the FTC takes a holistic approach to privacy regulation. The FTC believes that "generally applicable laws are needed to ensure appropriate protections for consumers' privacy and data security *across the marketplace*."[53] Likewise, the Industry Framework explained that its approach "will ensure that the same privacy and security framework applies to all entities in the Internet Ecosystem" in order to "minimize customer confusion as well as other harms associated with disparate privacy regulation across the ecosystem"[54]

The Multicultural Media, Telecom and Internet Council and its diverse coalition of civil rights, civic and government organizations ("MMTC") stated that the "NPRM's construct is too complicated and too narrowly focused on a consumer consent regime targeted solely to [ISPs] within the broader Internet ecosystem."[55] The Electronic Privacy Information Center ("EPIC") agreed that the rules proposed in the *NPRM* are too narrow and should be extended to other players in the Internet ecosystem, stating that:

> [t]he current description of the problem presents ISPs as the most significant component of online communications that pose the greatest threat to consumer

[53] FTC Staff Comments at 8 (emphasis added).
[54] Industry Framework.
[55] Comments of Comments Of The Multicultural Media, Telecom And Internet Council, *et al.*, WC Docket No. 16-106 (filed May 27, 2016) ("MMTC Comments") at 2.

> privacy. This description is inconsistent with the reality of the online communications ecosystem, incorrectly frames the scope of communications privacy issues facing Americans today, and is counterproductive to consumer privacy.[56]

Five National Diverse Chambers of Commerce ("NDCC"), which represent nearly 10 million minority-owned small- and medium-sized businesses across the U.S., agree with the Commission that "consumers should be able to access information without the threat of unwarranted data collection."[57] However, NDCC correctly observed that the proposal "to treat [ISPs] differently than other Internet companies nullifies this objective by fostering an immense amount of confusion. Ultimately this leaves consumers unprotected by the biggest users of their data online."[58] NDCC also expressed concern about the potential for digital redlining by "big tech," namely large Internet companies "whose business models are based on data collection and monetization of such data through targeted advertising."[59]

C. The Commission Should Adopt The FTC's Definition Of Personally Identifiable Information.

The FTC correctly characterized the Commission's proposal to include *any* consumer data that is linkable as an unnecessary limitation on the use of data that does not pose a risk to consumers.[60] The FTC therefore recommended that the definition of PII should only include information that is "reasonably" linkable to an individual.[61] WISPA agrees with this recommendation, which helps address concerns that the proposed definition of PII is too broad, resulting in unreasonable and costly regulatory requirements to protect or restrict use of PII that

[56] EPIC Comments at Exhibit 3, 1-2.
[57] Comments of Michelle Dhansinghani (on behalf of five major National Diverse Chambers of Commerce in the United States, WC Docket No. 16-106 (filed May 27, 2016) ("NDCC Comments") at 1.
[58] *Id.*
[59] *Id.*
[60] FTC Staff Comments at 9.
[61] FTC 2012 Report "Protecting Consumers Privacy in an Era of Rapid Change" at 18.

poses little or no risk to consumers.[62] Adopting the FTC's recommendation will help reduce the types of PII or other data that is restricted from use or subject to security breach notification.

D. The Record Reflects The FTC's Concern Regarding The Commission's Proposed Customer Approval "Opt-In" Framework.

The FTC Staff Comments raise issues regarding the Commission's proposal that certain forms of consent are required based on the entity collecting the data, rather than on the sensitivity of the data and how the information is shared. The FTC explained that "[t]he FTC's general approach to consumer choice has focused on whether the collection and use of information is consistent with the context of a consumer's interaction with a company and the consumer's reasonable expectations."[63] The record favors this consumer-focused approach,[64] not the Commission's proposed opt-in framework.[65]

The Commission's proposed approach does not take into account the sensitivity or confidentiality of consumer's PII, and thus "does not necessarily reflect consumer's privacy preferences."[66] By contrast, the FTC's framework "focuses the sensitivity of consumer data and particular promises made about data collection and use, rather than on what type of entity collects or uses the data. The FTC recommends opt-in consent for unexpected collection or use of customers' sensitive data such as Social Security numbers, financial information, and

[62] *See* WISPA Comments, at 19-24. *See also* Comments of the Information Technology Industry Council, WC Docket No. 16-106 (filed May 27, 2016) ("ITI Comments") at 13; Comments of AT&T Services Inc., WC Docket No. 16-106 (filed May 27, 2016) at 75; USTelecom Comments at 6-8.
[63] FTC Staff Comments at 19.
[64] *See* ITI Comments at 7-8; Comments of Hance Haney Senior Fellow Discovery Institute, WC Docket No. 16-106 (filed May 27, 2016) at 6; Sprint Comments at 8-9; Reply Comments of the Association of National Advertisers, WC Docket No. 16-106 (filed July 5, 2016) at 5.
[65] *See NPRM* at 2538.
[66] Ohlhausen Remarks at 4.

information about children."[67] The FTC does not support the Commission's more expansive view, which would burden providers without benefiting consumers.

Instead of its proposed customer approval opt-in framework, the Commission should adopt the long-standing privacy practice that opt-in requirements are based on the sensitivity of the data and how the data is shared, rather than on the entity that is using or collecting the data. Alternatively, if the Commission rejects the FTC's approach, the Commission should exempt small broadband providers from its proposed customer approval framework altogether. Such action would be consistent with the record. ACA asked the Commission to "exempt small providers from the requirement to obtain additional customer approval to use, disclose, or make available customer proprietary information, provided they do not share sensitive information with unaffiliated third parties for marketing purposes."[68] Similarly, RWA "strongly supports an exemption from customer approval provisions for small BIAS providers, provided they do not share customer data with third parties."[69] NTCA proposed that "small providers should be governed by an opt-out approval process to the extent that any disparate treatment is bestowed upon various actors in the industry."[70] WISPA agrees that if the FTC approach is not adopted, small providers should be exempt from opt-in customer approvals, provided that they do not share the information with unaffiliated third parties for marketing purposes.

In sum, WISPA and other commenters do not dispute that consumers should receive basic protections for their online communications. However, such protections must be reasonable, reflect the reality of how the Internet works and address what consumers prefer, and should not impose regulations that are unnecessary to achieving legitimate public interest

[67] *Id.*
[68] ACA Comments at 45.
[69] RWA Comments at ii.
[70] NTCA Comments at 50-51.

objectives. The FTC's recommendations wisely suggest a reasonable approach that balances the interests of consumers and the obligations of industry.

E. The FTC's Concerns Regarding The Proposed Security Breach Notification Rules Are Shared By WISPA And Other Commenters.

The FTC shares WISPA's concerns and those of a number of commenters that the Commission's proposed data breach notification rules are flawed. These concerns include the proposed broad and overinclusive definition of "breach," strict liability notification requirements absent a "good faith" exception, the absence of a reasonable notification trigger, and unrealistic deadlines for notifying the Commission, law enforcement and consumers.[71] For example, ACA stated that the Commission should replace its specific rules with best practices.[72] Sprint emphasized that "[a]ny notice requirements, however, must be fine-tuned to ensure that customers, law enforcement, and other stakeholders, receive appropriate and accurate notice calibrated based on the scope of breach, including the reasonable risk of harm and the sensitivity of the data at issue, as well as the notice content and timing."[73] ITI explained that "the FCC proposes to regulate breach notification in a way that is contrary to the existing notification regimes as well as the proposals under consideration by Congress."[74]

WISPA agrees that the proposed definitions and rules for data breach notifications are unrealistic. Following are specific recommendations on how the rules can better reflect business realities and consumer expectations.

---

[71] *See* FTC Staff Comments at 30-32; and WISPA Comments at 18-23. *See also* ITI Comments at 11-12; ACA Comments at 53; CTIA Comments at 179-80; Comments of Competitive Carriers Association, WC Docket No. 16-106 (filed May 27, 2016) ("CCA Comments") at 45; Comments of State Privacy and Security Coalition, WC Docket No. 16-106) ("SPSC Comments") at 14.
[72] ACA Comments at 53.
[73] Sprint Comments at 15.
[74] ITI Comments at 12.

Definition of Security Breach.

The Commission's overly broad security breach notification proposal requires notification to a consumer in "*any* instance in which a person, without authorization or exceeding authorization, has *gained access to*, used, or disclosed customer proprietary information."[75] Unlike existing Section 64.2011 under the Commission's CPNI rules, which is limited to intentional security breaches,[76] the proposed definition would extend to *unintentional* breaches, including access without any use or disclosure, and covers all customer proprietary information, not just CPNI.[77]

This proposal is unworkable on several levels. First, as the FTC explained, the proposed notification requirement would apply when there is unauthorized access to *any* customer proprietary information, which would in effect require a broadband provider to collect and retain more customer proprietary information than should be necessary.[78] The FTC Staff Comments and others illustrate the burden on those broadband providers that would be prohibited from collecting only a persistent identifier or information held in cookies because the provider would also need to collect and retain an email address to comply with the proposed notice requirement.[79] Second, similar to WISPA's Comments, the FTC correctly observed that an actual or alleged breach of a persistent identifier, without more, does not raise the same risk of harm as a breach of more sensitive information.[80] Third, as WISPA and others stated,[81] mere access to private information (however defined) does not result in consumer harm; harm arises only when the information is used or disclosed in ways that exceed the scope of the consumer's

[75] *NPRM* at 2525-2526 (emphases added).
[76] 47 C.F.R. § 64.2011.
[77] *See NPRM* at 2526.
[78] *Id*.
[79] FTC Staff Comments at 31. *See also* ITI Comments at 13, Verizon Comments at 35, 40-21.
[80] *See id.* at 31. *See also* WISPA Comments at 23.
[81] *See* WISPA Comments at 22; ACA Comments at 55; CTIA Comments at 87; SPSC Comments at 2.

approval. Fourth, as many commenters pointed out,[82] unintentional breaches should not trigger a data breach notification, unless there is actual consumer harm. Adopting rules that require notice of intentional breaches for the actual and unauthorized use or disclosure of CPNI would appropriately trigger notification only in cases of actual consumer harm and relieve broadband providers from unnecessary and burdensome obligations that are inconsequential for consumers.

Over-Notification and Notice Fatigue.

The FTC's second concern regarding the Commission's proposed security breach notification requirements is the risk of consumer over-notification to consumers.[83] The Commission has acknowledged that over-notification results in "notice fatigue,"[84] an issue also raised by WISPA.[85] Consistent with this view, the FTC Staff Comments emphasize that not every form of customer proprietary information should be subject to notification and not every instance of a security breach as defined by the Commission should trigger the notification requirement.[86] To quote the FTC, "when consumers receive 'a barrage of notices' they could 'become numb to such notices, so that they may fail to spot or mitigate the risks being communicated to them.'"[87] The FTC therefore proposed that the Commission's proposed notification rules be limited "to a narrower subset of personal information than customer proprietary information and not include device identifiers, cookies, or other persistent identifiers, standing alone."[88]

---

[82] *See* WISPA Comments at 22; ACA Comments at 55-56; CTIA Comments at 175; NTCA Comments at 67; Comments of WTA – Advocates for Rural Broadband, WC Docket No. 16-106 (filed May 27, 2016) ("WTA Comments") at 8-9.
[83] FTC Staff Comments at 31.
[84] The FCC defines the concept of "notice fatigue" as "the harms inherent in over-notification" and mentions it several places throughout the *NPRM*. *See NPRM* at 2509, 2550, and 2567.
[85] FTC Staff Comments at 31. *See also* WISPA Comments at 7.
[86] *Id.* at 30.
[87] *Id.* at 31 (*citing* FTC Statement of Basis and Purpose to its Health Breach Notification Rule, 74 Fed. Reg. at 42963).
[88] *Id.* at 32.

In addition, to help avoid "notice fatigue," the FTC also supported the "good-faith" exemption from notification for certain inadvertent access by company employees.[89] The FTC's position is strongly supported by various other commenters. For example, CTIA stated that "the Proposed Notice Rules could require frequent and intrusive notices to consumers, increasing the risk that customers will experience notice fatigue and possibly fail to appreciate the most important notices that impact customer privacy."[90] ITI stated that "[i]f over-notification becomes commonplace, consumers will have difficulty distinguishing between notices, and determining which one warrant them to take action."[91] CCA similarly stated that "'notice fatigue' is antithetical to consumer protections, and would make it less likely that consumers become aware of truly alarming data breaches."[92] Other commenters provided useful statistics regarding the effects of "notice fatigue."[93] Several commenters also expressed that "just in time" notices and approvals would be extremely burdensome for consumers and contribute to "notice fatigue."[94] The Commission must consider the fact that over-notification can lead to customers undermining the trust of broadband providers.[95]

WISPA supports the FTC's recommendations on a refined scope of the security breach notification requirements and the need to include a good faith exception, and also recommends

---

[89] *Id.*
[90] CTIA Comments at 100. CTIA further explained that "[t]hese predictions are not mere speculation; they find support from scientific studies, which demonstrate that consumers are not served by expansive, untimely, and repetitious privacy notices. Further, data from Europe suggest that providing customers with frequent notices results in customer annoyance and many even deter customers from visiting certain websites." *Id.* (citations omitted).
[91] ITI Comments at 11.
[92] CCA Comments at 44.
[93] *See* Comments of The Center for Democracy & Technology, WC Docket No. 16-106 (filed May 27, 2016) ("CDT Comments") at 23 ("The average consumer would need to spend between 181 and 304 hours each year reading web site privacy policies to be able to understand how their information is being used."); EPIC Comments at 6 ("It would take 76 working days to read the privacy policies they [consumers] encounter in one year" and "[i]f consumers were to actually ready every privacy policy, the opportunity cost to the national economy would be $781 billion").
[94] *See* USTelecom Comments at 12; NTCA Comments at 54; Comments of CenturyLink, WC Docket No. 16-106 (filed May 27, 2016) at 43; Comments of CompTIA, GN Docket No. 16-106 (filed May 27, 2016) at 5; ACA Comments at 37; WTA Comments at 14-16.
[95] ACA Comments at 21.

that security breach notification requirements should apply only to sensitive PII.[96] This differentiation between sensitive PII and non-sensitive PII is an important distinction that many state and federal agencies make, including the FTC.[97] CTIA accurately pointed out that "[a]s the FTC explained, while the misuse of sensitive data can increase the likelihood of 'embarrassment, discrimination, or other harms, *there are fewer privacy risks associated with the use of non-sensitive data*."[98] As SPSC stated, "the NPRM proposal is broader than existing information security and breach notice requirements in that it would apply to a large range of information that is not sensitive, including even data that is publicly available or that travels widely around the Internet when users communicate."[99] WISPA also agrees with CCA that the Commission should seek further comment on the scope "highly sensitive information," which CCA proposes to define as "sensitive personal information not available through public means, if released, would cause material harm to the individual."[100]

By contrast, EFF argued that "defining categories of 'sensitive' information may create a perverse incentive for BIAS providers to identify or inspect protected data in order to determine whether it falls into a 'sensitive' category."[101] Such suspicions are unfounded. First, as explained elsewhere in these Reply Comments, many small broadband providers do not have the means or time to collect, inspect and assess data in this way. Second, distinguishing between sensitive and non-sensitive information allows providers to ensure greater protection of the

[96] WISPA Comments at 23 ("customers would, under the Commission's regime, receive notices that have no bearing on whether a breach is likely to subject the consumer to identity theft or other similar harms" and the "Commission should separate non-sensitive data from sensitive data, and treat them differently").
[97] *Id.* at 22. *See also* CTIA Comments at 97 ("most state data breach notification laws are triggered by a likelihood of harm to consumers, which is generally tied to the sensitivity of the data at issue").
[98] *Id.* at 97 (emphasis added).
[99] SPSC Comments at 2.
[100] CCA Comments at 26.
[101] EFF Comments at 5.

sensitive information, not less. Therefore, "companies should have fewer regulatory obligations when they provide notice and choice regarding non-sensitive information."[102]

Data Breach Notification Deadlines.

The FTC Staff Comments also questioned the Commission's proposed seven-day deadline for notice of a security breach to the Commission and law enforcement, and the ten-day notice deadline to consumers, explaining that these deadlines are "too short and may not allow companies sufficient time to conduct an investigation."[103] Significantly, the FTC stated that "[t]his could have a detrimental effect on consumers, who could get erroneous information about breaches."[104]

WISPA and other broadband providers share the FTC's concerns regarding the Commission's proposed data breach notifications deadlines.[105] CTIA recognized that "the timelines for breach notification set forth in the *NPRM* are unrealistic. It is generally difficult to know the scope of the breach, the affected parties, and nature or potential risk of harm, within 7 to 10 days."[106] ITI agreed that "[t]he proposal does not afford organizations adequate time to remediate any discovered vulnerabilities, or to conduct through investigations to ascertain the nature and scope of any breach, before notifying customers or government agencies of a breach of data."[107] CCA explained the harms of rapid notification deadlines, observing that the "BIAS provider may not have a full understanding of the extent of the breach, possibly resulting misleading, unnecessary incomplete notifications, and consumer confusion."[108] SPSC noted that "[a] 10-day notice requirement to customers is without precedent even in the current CPNI rules

[102] CTIA Comments at 97.
[103] FTC Staff Comments at 32-33.
[104] *Id*. at 33.
[105] *See* WISPA Comments at 32.
[106] CTIA Comments at 179-80.
[107] ITI Comments at 12.
[108] CCA Comments at 45.

and does not provide businesses with nearly enough time to conduct a thorough and accurate investigation" and that "[c]omplicated breaches may take well over a month to investigate properly."[109] The Commission's proposed timeframe is also contrary to President Obama's remarks at the Cybersecurity and Consumer Protection Summit at Stanford University in which he called for a "single national standard so Americans know within 30 days if your information has been stolen."[110]

Not surprisingly, public advocacy groups have a different perspective. For example, New America asserted that "BIAS providers should… notify customers under the timetable proposed, not 'without unreasonable delay' or as 'expeditiously as possible" because "[s]uch unclear deadlines…would increase the likelihood of harm to customers and complicate a straightforward requirement that is not unduly burdensome."[111] Notably, this statement comes from a commenter that cannot understand the burdens of meeting such a rigid deadline in a real-world business context and has limited, if any experience, in working through the difficulty of investigating an actual or alleged data breach to determine the cause, the persons who may be affected, and the short and long-term solutions to mitigate consumer harm.

To resolve its concerns regarding the short deadlines for notification, the FTC recommended that companies be required to provide breach notices "without unreasonable delay, but not later than an outer limit of between 30 and 60 days."[112] This recommendation would align with several commenters' proposals that broadband providers should provide notice of a

[109] SPSC Comments at 14. SPSC also explained how the Commission's proposal is contrary to state laws and that "[t]he shortest state notice deadline to affected individuals is 30 days with a 15 day extension, and that law is an outlier in state data breach law." *Id.*, *citing* Fla. Stat. §501.171). For example, the CTIA Comments note that the Office of Personnel Management (OPM) "… initially identified a breach in early 2015 and then identified another breach in June 2015. For this second breach, OPM did not even start to notify affected individuals until September 30 and then continued for approximately three months. *See* CTIA Comments at 181.

[110] ACA Comments at 35- 36 *citing to* President Barack Obama, Remarks of Cybersecurity and Consumer Protections Summit, Stanford University, Feb. 13, 2015.

[111] New America Comments at 43.

[112] FTC Staff Comments at 33.

data breach "as soon as practical."[113] The FTC's proposal also would avoid conflict between federal and state data breach notification laws. ACA pointed out that currently "only eight states require notification within a specific time frame, and most of those states provide 45 days or more to provide notice."[114] WISPA agrees with the practical approach the FTC has recommended.

Further, the record supports WISPA's proposal that notifications of data breaches should be triggered when there is a "risk of harm."[115] The FTC's proposal to include a good faith exception supports and is consistent with a "risk of harm" trigger. In recommending the same approach, SPSC indicated that "[a] large majority of state breach notice laws (41 out of 47) contain a 'harm trigger' to distinguish between these circumstances and to avoid over-notification."[116] CTIA pointed out that "the Proposed Rules would conflict with many of the intent and harm requirements in these [state] laws and certainly complicates compliance by adding another set of requirements to follow."[117] The Commission should follow the record and limit notifications only to instances of consumer harm.

III. THE RECORD DEMONSTRATES THAT IMPLEMENTING CERTAIN PROPOSED BROADBAND PRIVACY RULES WOULD BE CONTRARY TO THE PUBLIC INTEREST.

A. The Proposed Definition Of "Customer" Is Overbroad And Should Only Include Current Customers.

WISPA and a number of other commenters showed that the Commission's proposal to define a "customer" as a current customer, former customer, or an applicant would be

[113] *See* WISPA Comments at 32 (proposing "as soon as practicable under the circumstances" for small providers); ACA Comments at 55 (proposing "as soon as reasonably practicable").
[114] *Id.* at 55 and n.100.
[115] WISPA Comments at 23. *See also* NTCA Comments at 67; ACA Comments at 34 and 55; WTA Comments at 9.
[116] SPSC Comments at 13.
[117] CTIA Comments at 183. CTIA also properly noted that "the Commission should be clear about the extent to which it would preempt state law requirements." *Id.*

unnecessarily overinclusive.[118] With respect to former customers, WISPA observed that "there are already other federal and state laws that govern these business relationships, and there is no need for the Commission to create redundant and confusing regulations here."[119] Former customers should be excluded because "[a]ny data associated with the former customer that is eligible for protection under the CPNI rules would have originated during the time of the provider-customer relationship and, therefore, would already be protected based on the provider's ongoing duty."

WISPA also stated that the term "applicant" should not be included in the definition of "customer" because "under Section 222 and existing Commission rules, a 'customer' is a person or entity to which a telecommunications company is *currently* providing service."[120] Sprint explained that applicants "neither use the broadband connections that are the subject of the Commission's rules, nor do they provide data implicated by the application of Section 222."[121] Likewise, CTIA noted that the proposed inclusion of applicants would "needlessly complicate ISPs' abilities to sign up prospective subscribers, and would create cumbersome requirements that would confuse and annoy current and prospective customers."[122] Further, applicants will have express notice from the broadband provider by way of a posted privacy policy that explains how information can be used. WISPA agrees with Sprint's recommendation that the Commission should limit "customer" to "a current account holder to ensure that any final rules are appropriately tailored to address the privacy concerns that are the focus of this proceeding."[123]

---

[118] *See* WISPA Comments at 23; ITTA Comments at 21; CCA Comments at 36; CTIA Comments at 95.
[119] ACA Comments at 45
[120] WISPA Comments at 23-24, *citing NPRM* ¶ 31, ¶ 32, *citing* 47 C.F.R. § 8.2(a); and *2015 Open Internet Order* at 5682-86, ¶¶ 187-93.
[121] Sprint Comments at 3.
[122] CTIA Comments at 95.
[123] Sprint Comments at 3.

By contrast, New America argued that "[i]ncluding only current customers would be too narrow because of the strong incentives for BIAS providers to collect and retain data from all customers without limitation."[124] WISPA strongly disagrees. First, as stated above, expanding the definition of "customer" to include both former customers and applicants will impose impractical regulations on providers. Second, many small providers do not collect and retain data on their former customers and applicants, or even their current customers, which moots the issue and makes any expansion of the definition of "customer" unnecessary.[125]

B. The Commission Should Not Prohibit Deep Packet Inspection.

Broadband providers sometimes use deep packet inspection ("DPI") for network management and other purposes.[126] According to WTA, "deep packet inspection has legitimate network management purposes such as use in resolving congestion issues, addressing distributed denial of service attacks, and resolving issues that arise in telecommunications networks."[127] Other legitimate uses include improving perceived customer performance and enforcing and/or correcting poor application behavior.

Certain commenters, however, seek to prohibit DPI, contending, in the words of EFF, that DPI "represents a direct threat to consumers' legally protected privacy because it allows carriers to exploit their unique choke point position as gatekeepers to capture all consumer activity online."[128] New America alleged that "DPI can reveal extremely sensitive information about BIAS customers' online activities and communications, including content" and argued that

[124] New America Comments at 14.
[125] *See* NTCA Comments at i; RWA Comments at i, 5; WTA Comments at iii, 2.
[126] *See NPRM* at 2581.
[127] WTA Comments at 23-24. *See also* EFF Comments at 10.
[128] EFF Comments at 10 (citation omitted).

DPI should be prohibited or otherwise subject to a heightened approval framework.[129] EPIC stated that DPI must be prohibited[130] because it is "highly intrusive surveillance" and that "consumers should not be permitted to consent to DPI because it can collect communications from third parties who have not consented to this invasive surveillance."[131]

These comments miss the point – it is not the fact of DPI that may be arguably troublesome, but how information obtained through DPI may be used to harm consumers' legitimate privacy interests. Rather than implementing an outright ban, the Commission should follow the approach it took in the *2015 Open Internet Order* and permit DPI for "reasonable network management purposes" and, if disclosed and approved, for other purposes.[132] There should be no flat ban on DPI, which can be an essential tool for some providers to address risks to their networks from viruses and malware and to manage traffic flows with dissimilar requirements.[133] As Verizon stated, "so long as customers are given notice about a broadband provider's practices and a fair opportunity to consent to the practice, there is no reason for this rigid, categorical ban."[134] To the extent a provider does not follow its own disclosed policy or otherwise uses DPI to violate other Commission rules, there are enforcement remedies that will suffice.

C. The Record Demonstrates Strong Support For A Multi-Stakeholder Process.

WISPA and other commenters urged the Commission to use a multi-stakeholder process to develop industry standards and safe harbors.[135] WISPA's participation on the Consumer

[129] New America Comments at 23. *See also* Comments of Public Knowledge, *et al.*, WC Docket No. 16-106 (filed May 27, 2016) ("Public Knowledge Comments") at 24-25 (DPI should be opt-in only).
[130] EPIC Comments at 10-11.
[131] EPIC Comments at 26.
[132] *See 2015 Open Internet Order* at 5677, 5733.
[133] *See, e.g.,* WTA Comments at 23-24. *See also* EFF Comments at 10.
[134] Verizon Comments at 43.
[135] *See* WISPA Comments at 16; MMTC Comments at 2; ACA Comments at 5. *See also* CCA Comments at 41.

Advisory Committee ("CAC") has provided WISPA with insight into the benefits of cooperative, consumer-driven, provider-informed best practices that can be balanced with the capabilities of providers. WISPA agrees with FPF that "[i]t is important that multi-stakeholder processes be driven by the stakeholder community, with the government's most helpful role as facilitator and fair broker."[136]

Conversely, Consumer Watchdog stated "[t]here is no useful purpose to a 'multi-stakeholder' process" and claims that the Department of Commerce's multi-stakeholder proceedings regarding the privacy of mobile apps were "largely captured by industry" and that "consumer and privacy advocates were so disappointed with the facial recognition that they withdrew."[137] This has not been the experience of WISPA with respect to its participation on both the CAC and in the Wireless Innovation Forum, which is developing spectrum management standards for the Citizens Broadband Radio Service. In addition to these experiences, USTelecom lists examples of successful multi-stakeholder initiatives – NIST, CSF, CSRIC Working Group 4 – all of which when "taken together represent a significant commitment by the Communications Sector in resources, time and energy and flow from the belief that the US government and its agencies can be trusted to support a partnership-based approach as a foundational national policy matter."[138]

---

[136] Comments of Future of Privacy Forum, WC Docket No. 16-106 (filed May 27, 2016) at 33. In fact, President Obama's Privacy Blueprint observed that "open, transparent multi-stakeholder forums can enable stakeholders who share an interest in specific markets to business contexts to work toward consensus on appropriate, legally enforceable codes of conduct." *Id.* at 32-33 (citation omitted).

[137] Consumer Watchdog Comments, WC Docket No. 16-106 (filed May 27, 2016) at 7. While some consumer groups criticized NTIA's multi-stakeholder process for mobile app privacy, others were supportive. "Pam Dixon of the World Privacy Forum, who is historically critical of self-regulatory efforts in general, participated in the process and said it changed her perspective. Rather than being industry-driven, consumer input was considered and compromises were reached." Angelique Carson, CIPP/US, *Did NTIA's Multi-Stakeholder Process Work? Depends On Whom You Ask*, IAPP Privacy Advisor (Sept. 3, 2013). Moreover, the art of a true multi-stakeholder process is when various stakeholders have compromised to meet a consensus. "With that many diverse groups working together . . .certainly there are bound to be people who are not satisfied with particular outcomes, but that's part of the nature of compromise." *Id.* (*quoting* NTIA's John Verdi, Facilitator).

[138] USTelecom Comments at 25.

D. The Commission Should Adopt A "Safe Harbor" For Privacy Notices.

WISPA[139] and a number of other commenters including NTCA,[140] RWA[141] and ACA[142] supported privacy notice "safe harbors" to encourage uniformity in the way privacy policies are presented to consumers and to provide a measure of certainty that the "safe harbor" can act as a defense. As EFF stated, "regarding the format of BIAS providers privacy policies, it is clear that the development of a standardized template for disclosure that can serve as a safe harbor will help to ease the regulatory burden on BIAS providers, and could also help customers better understand BIAS provider privacy practices."[143] The "safe harbor" should be developed by a multi-stakeholder group such as the CAC.

IV. THE RECORD DEMONSTRATES THAT THE HARMS OF THE PROPOSED BROADBAND PRIVACY RULES WOULD OUTWEIGH THE BENEFITS FOR SMALL BROADBAND PROVIDERS AND THEIR CUSTOMERS.

A. The Commission Failed To Comply With The Regulatory Flexibility Act.

In its Reply Comments, Advocacy points out that the IRFA does not comply with the provisions of Section 607 of the Regulatory Flexibility Act ("RFA"), which requires agencies to "provide either a quantifiable or numerical description of the effects of a proposed rule or alternatives to the proposed rule, or more general descriptive statements if quantification is not practicable or reliable."[144] Rather, as Advocacy observes, "the FCC simply describes compliance requirements and seeks comment on compliance costs, without making any attempt to explain what kind of costs small BIAS providers might incur in order to comply, and without

[139] *See* WISPA Comments at 16.
[140] *See* NTCA Comments at 35, 41, 54, and 56.
[141] *See* RWA Comments at 7 (standardized privacy disclosure as a volunteer safe harbor).
[142] *See* ACA Comments at 50 (standardized notices provide a safe harbor).
[143] EFF Comments at 13.
[144] *See* Advocacy Reply Comments at 2, *citing* 5 U.S.C. § 607.

any discussion of how those costs might be disproportionately burdensome for small entities."[145] It is not enough for the Commission to merely cite the rule and state that it "expects to consider the economic impact on small providers, as identified in comments filed in response to the Notice and this IRFA, in reaching its final conclusions and taking action in this proceeding."[146]

B. Small Businesses Will Be Harmed By The Proposed Rules.

WISPA's Comments make clear that small broadband providers lack the resources that would be required to comply with the Commission's detailed and prescriptive regulatory scheme, and ultimately would be harmed by the proposed rules.[147] Other commenters representing small entities, including Advocacy, share the same concerns regarding the limitations of small businesses and how unintended consequences of the proposed rules would stifle broadband deployment.[148] Moreover, the record shows that small providers typically do not collect sensitive information from their customers for marketing purposes.

First, based on the record, and notwithstanding the Commission's abdication of its obligations under the RFA, it cannot be disputed that all broadband providers, large and small, would incur significant costs in order to comply with the Commission's proposed rules. Generally speaking, CTIA stated that the Commission's proposed risk management assessment and remediation mandate is "overly burdensome and unrealistic" and that "mandated

---

[145] *Id.* at 2-3.
[146] IRFA at ¶ 56. The IRFA cites to Part III.E.3 of the *NPRM*, which includes no reference to reducing burdens on small providers.
[147] *See* WISPA Comments at 26-34. Commenters generally oppose the Commission's suggestion to define a "small provider" as one with 5,000 or fewer customers, and suggest a higher number – up to 500,000 – as a definition that will better account for the compliance burdens presented in the *NPRM*, which "are far more onerous than the enhanced transparency requirements." CCA Comments at 32. *See also* USTelecom Comments at 19.
[148] *See generally* Advocacy Reply Comments. *See also* ACA Comments at iii, 21; SPSC Comments at 9; CCA Comments at 30, 31; CTA Comments at 10; Comments of Cincinnati Bell Telephone Company LLC, WC Docket No. 16-106 (filed May 27, 2016) at 10.

assessments are likely to cost millions of dollars and take substantial time."[149] AT&T observed that "the NPRM proposes a host of new information-collection obligations that would impose substantial burdens on ISPs of *every type and size* and that the NPRM falls far short of justifying the necessity for and practical utility of the proposed collections."[150]

For small providers, the burdens will be disproportionate. As a general proposition, and to paraphrase the maxim cited by Judge Williams, regulations are more burdensome for small companies than for large ones that can allocate fixed costs across a larger customer base.[151] That is clearly the case here – a mom-and-pop broadband provider with a handful of employees and a few hundred customers simply lacks the financial resources to establish compliance and reporting procedures, hire consultants to train staff and retain lawyers to address the heightened level of compliance risk they would face under the Commission's proposed rules. As USTelecom put it, "small providers would have unique challenges and an even greater burden attempting to implement the FCC's proposal rules."[152] CCA likewise stated that "small carriers simply do not have the resources, funds or staff to affordably implement the proposed rules, particularly when compared to larger providers"[153] and that "[m]any of the proposed rules would require significant resources to implement, to the detriment of competitive carriers and, ultimately, their customers."[154]

More specifically, ACA explained that the Commission's proposals would "impose tremendous burdens on providers," and described a long list of burdens including attorney and

[149] CTIA Comments at 163-64. CTIA also stated that ISPs will have to provide "an overwhelming number of notices" which will "generate substantial compliance and other administrative costs, which may ultimately be passed on to consumers as part of the cost of service." *Id.* at 100-101.
[150] AT&T Comments at 116 (emphasis added). AT&T indicated that the proposed rules would "subject ISPs to substantial operational costs, such as the cost of system changes and recordkeeping requirements" and that those costs would "skyrocket." *Id.* at 54.
[151] *See USTelecom* at 64-65 (Williams, J., dissenting).
[152] USTelecom Comments at iv.
[153] CCA Comments at 30.
[154] *Id.* at 16.

consultant costs; development and implementation costs; personnel costs; costs associated with all aspects of providing an required notices and follow-ups; third party costs associated with modifying contracts and ensuring compliance; and opportunity costs associated with diverting resources from innovation and infrastructure deployment.[155] ACA estimated that the costs of providing breach notifications and associated costs are "well over $130 per person."[156] Similarly, SPSC stated that breach notification incidents are expensive and that "[t]he average cost per record of a data breach including both out of pocket costs and harm to good will currently exceeds $200 per record."[157]

For a WISP with 500 subscribers, a $150 per-customer cost would amount to $75,000 per data breach incident – roughly the annual salary of a senior manager in a rural area, or the amount of investment needed to expand service to two additional tower sites to serve 500 new subscribers. In other words, the $75,000 compliance cost for one data breach incident would prevent a 500-customer WISP from having the financial ability to double the number of its subscribers, many of whom lack choice in broadband access.[158]

Second, in addition to the out-of-pocket cost, there is also the uncertain but inherent risk of enforcement that will chill investment or force providers – at least those who are financially able – to set up a "rainy day fund" instead of investing in network upgrade and expansion. CTA recognizes how the strict liability element of proposed Section 64.7005(a) could be a "death knell for smaller ISPs" because "[s]uch an unforgiving and unrefined standard could force an ISP

[155] ACA Comments at 23. *See also* Advocacy Reply Comments at 3 (listing costs "not limited to consulting fees, attorney's fees, hiring or training in-house privacy personnel, customer notification costs, and opportunity costs").
[156] ACA Comments at 35 and n.69 (citations omitted).
[157] SPSC Comments at 8, *citing* Ponemon Institute (2015), *2015 Cost of Data Breach Study: Global Analysis*.
[158] Another concern is the increased cost of insurance. A provider's errors and omissions insurance policy that covers data breaches is not likely to cover government fines, is already very expensive and is difficult for small businesses to obtain. Significantly expanding the scope of information that is considered private and dramatically increasing the compliance obligations make it more likely for a claim to be made and will result in the insurance becoming unattainable for smaller providers. This leaves smaller providers with a proportionally much greater risk than a large provider than can self-insure and/or absorb the significant risks and costs involved.

to spend scarce resources on efforts to encrypt large swaths of non-sensitive data to avoid the risk of being subject to an enforcement action by the Commission's Enforcement Bureau."[159]

Third, adopting the proposed regulatory scheme would create the perverse incentive of discouraging broadband deployment. SPSC recognized that the proposed rules would create "a strong incentive for business to prioritize protection of any information covered by a breach notice requirement over other information and network issues."[160] CTA stated that "[a]t a minimum, [the proposed data security rules] would deprive ISPs the right to make reasoned business decisions about their security choices and instead force them to divert precious time and money that could otherwise be spent on innovation and investment."[161] A poll of ACA members indicates that "across the board, the proposed rules will divert scarce resources from deployment, network improvement, and customer service to regulatory compliance."[162] ACA stated that "the proposed rules will have a significant impact on the ability of BIAS providers to offer market innovative services to their subscribers," which would eventually result in "fewer revenue opportunities that could support the deployment of broadband infrastructure."[163] CCA asked the Commission to adopt an exemption "that avoids placing small carriers in a position of choosing between investing in a needlessly complex and onerous framework instead of investing in their networks and improving broadband service in rural and regional parts of the country."[164]

Finally, the record shows that small broadband providers do not engage in data collection for third party marketing, which eliminates the need for any additional privacy regulations.[165] Public interest groups rationalize the need for addition ISP privacy regulations with the notion

[159] CTA Comments at 10.
[160] SPSC Comments at 9.
[161] CTA Comments at 10.
[162] ACA Comments at 21.
[163] *Id.* at 31.
[164] CCA Comments at 31.
[165] *See infra*.

that broadband providers hoard consumer information. New America opined that "BIAS providers can and likely do amass substantial data profiles that could represent years of intimate, personal, and sensitive behavioral information affecting millions of customers."[166] Free Press generally alleged that "ISPs track their customers, these companies create comprehensive profiles containing sensitive information on each person's finances, health, age, race, religion, ethnicity, and a host of other factors."[167] Taking it one step further, Public Knowledge posited that the cross-advertising business "has resulted in significantly enhanced revenue for BIAS providers."[168]

But none of these commenters provides any support for the proposition that small broadband providers engage in such tracking or profiling. To the contrary, the record makes clear that many small providers do not have the means or the incentive to collect information about their customers.[169] In addition, many small providers do not share customer information with third parties for advertising purposes, and if they do share information it is for the basic provision of telecommunications services.[170] The *NPRM* and the record are devoid of any evidence showing that there is a need to impose the same prescriptive regime on small providers that do not engage in the kinds of activities the Commission intends to regulate. "[T]he failure to recognize the differences in the scale and resources of regulated entities has in numerous instances adversely affected competition in the marketplace, discourage innovation and restricted

[166] New America Comments at 17.
[167] Free Press Comments at 5 (footnote omitted).
[168] Public Knowledge Comments at 9.
[169] *See* NCTA Comments at 1("NCTA members do not broker their customers' information"); RWA Comments at 5 ("small BIAS providers generally do not actively monitor, collect, or store such information because there is no business case to do so"); WTA Comments at 2 ("there is virtually no demand for most RLECs and their ISP affiliates to monitor the Internet browsing histories or online contacts of their customers").
[170] *See* RWA Comments at i ("BIAS providers like RWA's carrier members do not go to great lengths to collect, store, analyze, and exploit Customer Proprietary Information…for marketing purposes or other reasons"); WTA Comments at iii ("small telecommunications providers to date do not engage in the creation of highly detailed profiles of individual consumers or online behavioral advertising or retain substantial amounts of sensitive customer information"); CCA Comments at 4 ("small carriers need to share data and information with many vendors, affiliates and third parties on a daily basis to enable the provision of telecommunications").

improvements in productivity."[171] This is one of those instances. The actual and opportunity costs, the burdens of compliance and the risks of enforcement on small providers far outweigh any potential benefit to the public.

The Commission's proposals in this proceeding cannot be viewed in a vacuum. The proposed privacy and data security rules, the obligations under Title II, the potential sunset of the temporary small provider exemption on enhanced disclosure obligations and the new initiative to subject broadband providers to outage reporting rules will have a cumulative and devastating effect on small businesses. This unprecedented onslaught of new and inter-related regulatory obligations on a single class of small businesses not only contravenes the precepts of Section 257 of the Act and Section 706 of the Telecom Act, but will have dire consequences for small providers that will find it difficult, if not impossible, to survive. The Commission should not "regulate to death" small providers under a "one size fits all" regime in these proceedings.

C. Small Businesses Should Have Up To Two Years To Comply With Any New Rules The Commission Might Adopt.

As the record makes clear, small providers have limited financial resources and cannot be expected to immediately foot the bill for unbudgeted costs and expenses. Large companies may be in a position to absorb the additional costs with existing staff, but many small providers do not have in-house legal counsel and expertise to learn about the new requirements, implement compliance procedures and protect against enforcement and litigation risk. At a minimum, small providers will have to create new budgets to direct finite resources – in the neighborhood of $75,000 per breach incident for a provider of only 500 customers – away from maintenance, deployment, expansion and other activities to privacy compliance. Making this Hobson's Choice will take time.

[171] 5 U.S.C. §§ 601 *et seq.*, Congressional Findings and Declaration of Purpose, Sec. (a)(4).

Importantly, Advocacy "strongly supports suggestions that the FCC adopt delayed compliance schedules for small BIAS providers."[172] Advocacy recognized that "[g]iving small providers more time to comply with the FCC's rules will allow them to spread costs and manage their limited resources in a way that will minimize harm to their ability to service customers."[173] Other commenters agreed with WISPA that "small providers should be given up to two years after the effective date of any rules to meet any applicable new regulatory requirements."[174] RWA stated that "[a] 24-month compliance deadline extension would allow for small and rural BIAS providers to comply with the Commission's rules without unnecessarily expending resources on preparing and prosecuting a waiver request, while allowing them to continue to focus their resources on providing affordable, high-quality broadband that is necessary for economic development and public safety in rural areas."[175] ACA generally concurred, asking the Commission to "extend the compliance deadline for small providers by at least one year, with a subsequent rulemaking to determine whether to further extend the deadline and/or establish additional exemptions."[176]

While WISPA continues to believe that a two-year transition period is an appropriate period of time to budget and allocate for compliance, it does not object to the one-year period suggested by ACA so long as there is a further opportunity to determine whether the compliance deadline should be lengthened or broadened "in light of an adopted order, a refreshed record, and with the benefit of time and experience."[177]

[172] Advocacy Reply Comments at 4.
[173] *Id.*
[174] WISPA Comments at 28.
[175] RWA Comments at 8.
[176] ACA Comments at 46,
[177] *Id.* at 49.

D. Small Providers Should Be Permanently Exempt From Certain Requirements.

In its Comments, WISPA urged the Commission to afford small broadband providers to exempt small providers from certain rules.[178] Advocacy agreed, indicating its support for "exemptions for small BIAS providers wherever practicable."[179] Other commenters representing the interests of small providers asked the Commission to grant similar relief. For instance, ACA "respectfully calls on the Commission to adopt several targeted exemptions that will ease burdens on smaller providers while continuing to promote the Commission's goals of transparency, choice, and security.[180] Likewise, WTA "supports exemptions from the proposed new customer approval requirements, consumer data security requirements and data breach notification requirements for small RLECs and their ISP affiliates that do not collect or retain broadband usage information for marketing purposes of for sale to third-parties."[181] RWA similarly noted that, for small providers, "costs can be alleviated with targeted exemptions and compliance deadlines."[182]

Initial Comments supporting the proposed rules make sweeping arguments that do not distinguish between large and small providers and, presumably, favor a "one size fits all" approach. When weighed against the record to date, these Comments do not withstand scrutiny. The Commission should adopt the exemptions recommended by commenters so that small providers do not suffer the significantly disproportionate costs inherent in the far-reaching regulatory scheme the Commission has proposed.

[178] *See* WISPA Comments at 27.
[179] Advocacy Reply Comments at 4, *citing* ACA Comments at 8.
[180] ACA Comments at 44.
[181] WTA Comments at 2.
[182] RWA Comments at ii.

E. Existing Small Business Contracts Should Be Grandfathered From The Proposed Customer Approval Framework.

A number of commenters agree that "small providers should be permitted to grandfather existing customer approvals for the use and disclosure of proprietary information."[183] USTelecom supports "allowing small providers who have already obtained customer approval to use their customers' proprietary information to grandfather in those approvals for first and third party uses."[184] There does not appear to be objection in the record, and the Commission therefore should approve grandfathering.

Subjecting small providers to the proposed opt-in customer approval framework, as well as the proposed elimination of arbitration clauses,[185] will place undue burdens and costs on small providers. Requiring small providers to renegotiate and revise most of their existing agreements with operational service providers, third party vendors and customers also will require small providers to spend large amounts of time and money doing so. Most WISPs do not have dedicated in-house counsel, and will need to hire outside attorneys for both contract negotiations

[183] WISPA Comments at 31. See also ACA Comments at 45; USTelecom Comments at 19; WTA Comments at 16, CCA Comments at 33

[184] USTelecom Comments at 19. *See also* WTA Comments at 16 ("[t]o reduce the burdens on providers and to prevent customer frustration or fatigue, the Commission should grandfather existing opt-out approvals, at least for small providers already subject to CPNI rules"); CCA Comments at 33 (The Commission should "allow small providers who have already obtained customer approval to use customer PI, under their own privacy policies, to grandfather in those approvals, and be deemed in compliance with the new privacy regime"); ACA Comments at 45 (asking the Commission to "grandfather all existing consents between small BIAS providers and their customers, including those that permit sharing of customer information with third parties")

[185] *See NPRM* at 2546 and 2587. The record supports WISPA's position that arbitration and informal complaints should remain a method by which customers can seek resolution of their disputes. *See* WISPA Comments at 34; CTIA Comments at 50, nn.143 & 54; Verizon Comments at 76-78. Furthermore, that the length of time it takes to complete an arbitration is much shorter than litigation. The American Bar Association Section of Dispute Resolution ("ABA-SDR") reported that "the average time from commencement of a domestic, commercial arbitration to issuance of a final award ranges from 7 months to 7.3 months" while **"**in 2011, the median length of time from filing through trial of civil cases in the U.S. District Courts was 23.4 months and considerably longer in some of the busier courts." The ABA-SDR also reported that attorneys' fees and expenses are the most significant cost of litigation, and that "they increase in direct proportion to the time to resolution of the case." In addition, "[a]ttorneys' *fees and expenses can be minimized in arbitration* because arbitrations are generally concluded in far less time than cases in court." *See* ABA-SDR "Benefits of Arbitration for Commercial Disputes" at 3, *available at* http://www.americanbar.org/content/dam/aba/events/dispute_resolution/committees/arbitration/arbitrationguide.authcheckdam.pdf (last visited June 29, 2016).

and litigation. Further, small providers typically do not have much leverage with operational contracts and having to renegotiate previously agreed-upon contracts may put small providers at a significant disadvantage. Simply put, these additional costs could actually cripple many small providers.

F. The Proposed Data Protection Rule Should Be Revised To Accommodate Small Broadband Providers.

WISPA's Comments made specific proposals to amend proposed Section 64.7005 so that it would account for small broadband providers. Other commenters advocated a similar approach that considers the size of the provider. For example, NTCA urged the Commission to "*remain sensitive to the impact on small businesses*, whose networks may warrant a security approach different than that which would be more suitable to a larger firm, consistent with the voluntary, flexible, and scalable approach to cybersecurity as first espoused by the [Industry] Framework, and then subsequently by the Commission's CSRIC IV WG4."[186] Similarly, ITI emphasized that "risk management is a continuous process demanding flexibility in order to provide reasonable protections in light of the nature and scope of the activities of a given company, including the sensitivity of the data it handles, its threat profile, and *the size and complexity of the relevant data operations of the company*."[187]

To incorporate this principle and minimize the burdens on small providers,[188] the Commission should adopt a number of specific rules. First, as advocated in the WISPA Comments, the Commission should not apply proposed subsections (1)-(5) of Section 64.7005(a), as the specific requirements will be difficult, if not impossible, for small providers to

[186] NTCA Comments at 61 (emphasis added).
[187] ITI Comments at 15-16 (emphasis added).
[188] *See NPRM* at 2553.

meet.[189] In particular, the record reflects strong opposition to Section 64.7005(a)(3), which proposes that a broadband provider must "[d]esignate a senior management official with responsibility for implementing and maintaining the broadband provider's information security measures."[190] ACA stated that this proposed rule "would supersize the responsibility of the designated point of contact" to "effectively require a full-time staff member to manage privacy and data security compliance, which is well beyond the means of small providers."[191] ACA also pointed out that the average annual salary for a Chief Privacy Officer in the United States is $90,000, a cost many WISPs cannot afford (in fact, this annual salary may well be higher than the salary of the owner of a small WISP).[192]

Second, other commenters agree that if proposed Section 64.7005(b) is adopted, it should include an express recognition that the size of the provider should be considered in determining whether data security measures are "reasonably implement[ed]."[193] The proposed draft rule specifically takes into account "the nature and scope of the BIAS provider's activities" as well as "the sensitivity of the customer proprietary information held by the BIAS provider,"[194] but not the size of the provider, which directly affects the limits of compliance efforts. The size of the provider must also be taken into account because "even the proposed minimum data security standards would impose tremendous costs on small providers, which typically lack the resources

[189] *See* WISPA Comments at 31-32.
[190] *NPRM* at 2587. *See also* NTCA Comments at 63 ("the Commission should refrain from implementing requirements that speak to the specific credentials possessed by any senior manager," and that "[t]he Commission would be ill-placed to prescribe the various academic degrees or years of experience, or any other innumerable qualifications such a manager might be required to possess"); RWA Comments at 12 ("[s]addling small carrier employees with qualification requirements in rural markets (where workforce demands are often already difficult to meet) is counterproductive and may force small rural carriers into unnecessary additional hires, solely for the purpose of meeting such requirements"); WTA Comments at 23 (resource constrained RLECs have "small staff sizes and resources as compared to the salaries that full-time (or even part-time) experts can demand, as well as the lack of cybersecurity professionals in many rural areas").
[191] ACA Comments at 25.
[192] *Id.*
[193] *See* WISPA Comments at 31. *See also* RWA Comments at 10; ACA Comments at 44; WTA Comments at 21.
[194] *NPRM* at 2609.

and expertise of larger providers."[195] RWA plainly stated that "[i]f the Commission ultimately codifies a security requirement, it should take a BIAS provider's size and resources into consideration."[196]

Third, the record supports WISPA's position that small businesses should not be required to assume contractual liability for the data security practices of third parties. The record reflects that smaller providers do not have the same market power as the larger providers and may not be able to dictate contractual privacy terms the Commission deems necessary.[197] CCA explained that "any liability that a small carrier might be required to assume for third party actions that are likely beyond a carriers' control, might threaten the sustainability of that small business."[198] In addition, most small carriers do not have the litigation resources to enforce control of data.[199] Ultimately, third parties with which small providers contract are already subject to sufficient state and federal consumer protection laws, and the Commission has not sufficiently shown why it should impose additional rules.[200]

Conclusion

The Commission's proposals go too far. The Commission lacks statutory authority to adopt a regulatory regime that goes beyond the protection of CPNI. Even if the Commission has authority, the record demonstrates that the Commission should not exercise it in the prescriptive and heavy-handed way it proposes, but rather should take a more measured approach to privacy regulation. Small broadband providers will be disproportionately aggrieved if the Commission

[195] ACA Comments at 44.
[196] RWA Comments at 10 (citation omitted).
[197] *See id.* at 12-13.
[198] CCA Comments at 29. "Rules of this nature uniquely burden small and competitive carriers, which already have difficult time attracting the attention of device manufacturers and other major players in the telecom industry, and further discouraging those actors from dealing with small carriers is bad public policy." *Id.* at 40.
[199] *Id.*
[200] *See* RWA Comments at 13.

were to adopt the prescriptive, detailed and burdensome rules it proposes, many of which are unnecessary to protect broadband customers' legitimate privacy interests and would stifle – not encourage – broadband deployment to unserved and underserved Americans. These consequences are exacerbated by the combination of other regulations that do or will apply to newly minted Title II broadband providers – compliance with Open Internet rules, privacy and data protection rules and onerous outage reporting rules create a maelstrom of costly and burdensome that will challenge and cripple many small broadband providers. The Commission can mitigate these harms while protecting consumers by allowing small providers additional time to budget for the costs of compliance, grandfathering their existing privacy policies and exempting them from certain rules would help address the costs and burdens of compliance.

Respectfully submitted,

WIRELESS INTERNET SERVICE PROVIDERS ASSOCIATION

By: */s/ Alex Phillips, President*
/s/ Mark Radabaugh, FCC Committee Chair
/s/ Fred Goldstein, Technical Consultant

4417 13th Street #317
St. Cloud, Florida 34769
(866) 317-2851

Stephen E. Coran
S. Jenell Trigg
Deborah J. Salons
Lerman Senter PLLC
2001 L Street, N.W., Suite 400
Washington, DC 20036
(202) 429-8970
Counsel to the Wireless Internet Service Providers Association

July 6, 2016